Suricata NIDS Tools: Setup and Alert Workflow Report

Date : 08.5.2025

Prepared By: Aliu A. Sanusi

1. Summary

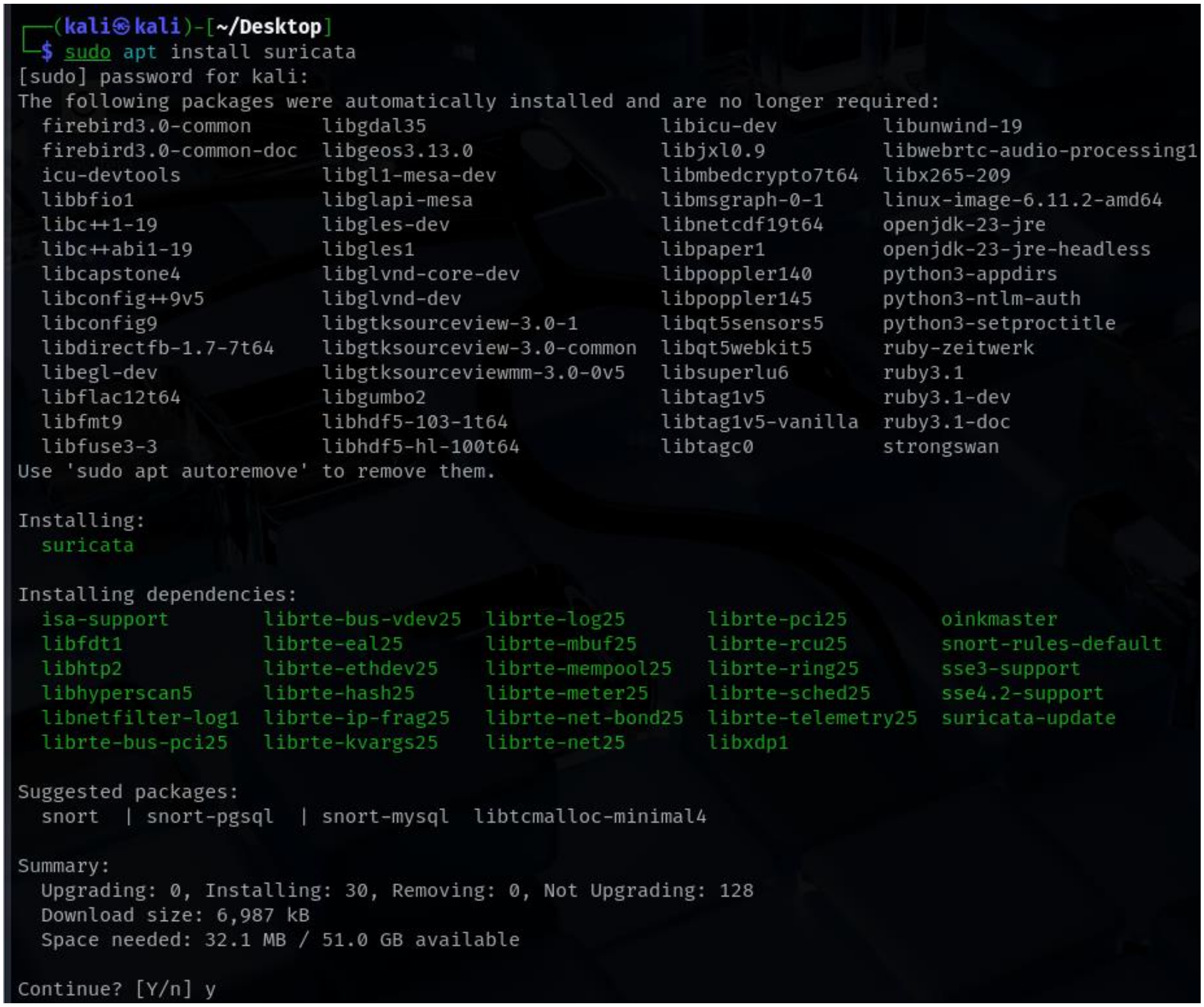
Suricata is an advanced, open-source network intrusion detection and prevention system (NIDS/NIPS) developed by the Open Information Security Foundation (OISF). It provides real-time packet analysis, protocol identification, and alert generation for suspicious network activity. This report outlines the steps to install, configure, and test Suricata, including the creation and verification of a custom detection rule.

2. Installing Suricata

Suricata must be installed on the target host system. Use the package manager appropriate for your operating system.

For Kali Linux/Debian:

```
sudo apt update sudo apt
install suricata
```

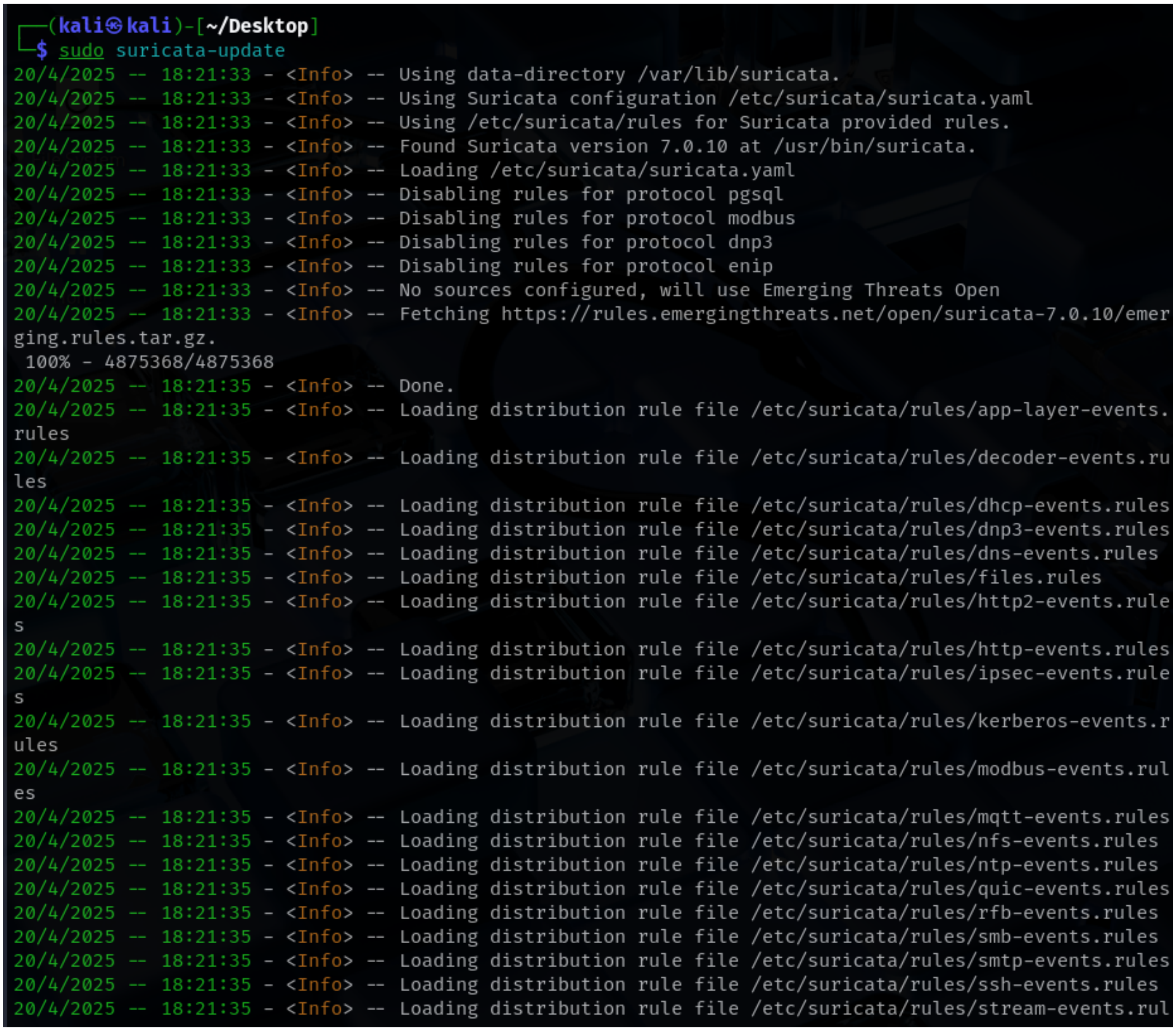


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install suricata
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  firebird3.0-common      libgdal35                    libicu-dev         libunwind-19
  firebird3.0-common-doc  libgeos3.13.0                libjxl0.9          libwebrtc-audio-processing1
  icu-devtools            libgl1-mesa-dev              libmbedcrypto7t64  libx265-209
  libbfio1                libglapi-mesa                libmsgraph-0-1     linux-image-6.11.2-amd64
  libc++1-19              libgles-dev                  libnetcdf19t64     openjdk-23-jre
  libc++abi1-19           libgles1                     libpaper1          openjdk-23-jre-headless
  libcapstone4            libglvnd-core-dev            libpoppler140      python3-appdirs
  libconfig++9v5          libglvnd-dev                 libpoppler145      python3-ntlm-auth
  libconfig9              libgtksourceview-3.0-1       libqt5sensors5     python3-setproctitle
  libdirectfb-1.7-7t64    libgtksourceview-3.0-common  libqt5webkit5      ruby-zeitwerk
  libegl-dev              libgtksourceviewmm-3.0-0v5   libsuperlu6        ruby3.1
  libflac12t64            libgumbo2                    libtag1v5          ruby3.1-dev
  libfmt9                 libhdf5-103-1t64             libtag1v5-vanilla  ruby3.1-doc
  libfuse3-3              libhdf5-hl-100t64            libtagc0           strongswan
Use 'sudo apt autoremove' to remove them.

Installing:
  suricata

Installing dependencies:
  isa-support        librte-bus-vdev25  librte-log25       librte-pci25         oinkmaster
  libfdt1            librte-eal25       librte-mbuf25      librte-rcu25         snort-rules-default
  libhtp2            librte-ethdev25    librte-mempool25   librte-ring25        sse3-support
  libhyperscan5      librte-hash25      librte-meter25     librte-sched25       sse4.2-support
  libnetfilter-log1  librte-ip-frag25   librte-net-bond25  librte-telemetry25   suricata-update
  librte-bus-pci25   librte-kvargs25    librte-net25       libxdp1

Suggested packages:
  snort  | snort-pgsql  | snort-mysql  libtcmalloc-minimal4

Summary:
  Upgrading: 0, Installing: 30, Removing: 0, Not Upgrading: 128
  Download size: 6,987 kB
  Space needed: 32.1 MB / 51.0 GB available

Continue? [Y/n] y
```

3. Updating Suricata

To ensure you have the latest threat detection capabilities, update the rule sets using `sudo`

```
sudo suricata-update
```



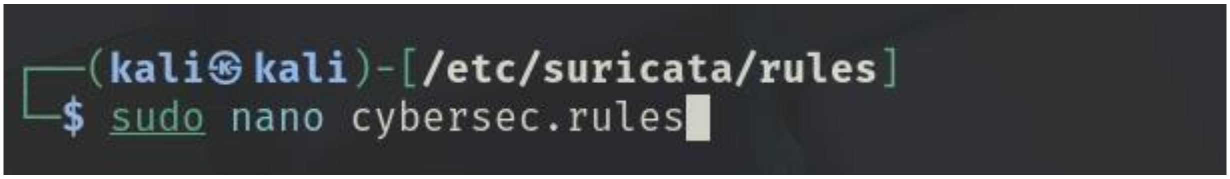
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo suricata-update
20/4/2025 -- 18:21:33 - <Info> -- Using data-directory /var/lib/suricata.
20/4/2025 -- 18:21:33 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
20/4/2025 -- 18:21:33 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
20/4/2025 -- 18:21:33 - <Info> -- Found Suricata version 7.0.10 at /usr/bin/suricata.
20/4/2025 -- 18:21:33 - <Info> -- Loading /etc/suricata/suricata.yaml
20/4/2025 -- 18:21:33 - <Info> -- Disabling rules for protocol pgsql
20/4/2025 -- 18:21:33 - <Info> -- Disabling rules for protocol modbus
20/4/2025 -- 18:21:33 - <Info> -- Disabling rules for protocol dnp3
20/4/2025 -- 18:21:33 - <Info> -- Disabling rules for protocol enip
20/4/2025 -- 18:21:33 - <Info> -- No sources configured, will use Emerging Threats Open
20/4/2025 -- 18:21:33 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.10/emer
ging.rules.tar.gz.
 100% - 4875368/4875368
20/4/2025 -- 18:21:35 - <Info> -- Done.
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.
rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.ru
les
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/http2-events.rule
s
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rule
s
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.r
ules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rul
es
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/mqtt-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/quic-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/rfb-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/ssh-events.rules
20/4/2025 -- 18:21:35 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rul
```

This command downloads current community rules, such as those from Emerging Threats.

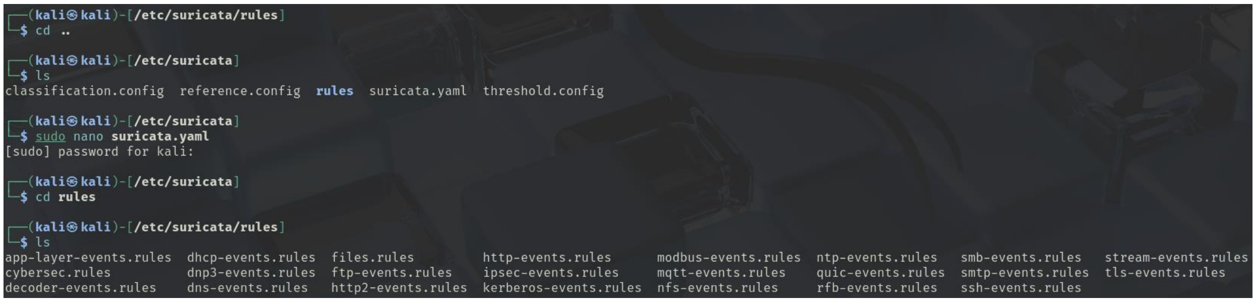
4. Setting a New Rule Destination

Custom rules are typically stored in:

```
/etc/suricata/rules/
```



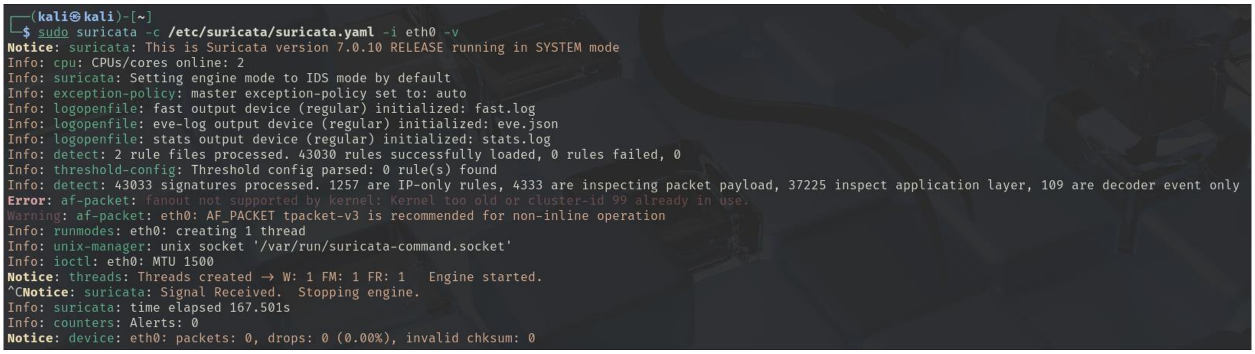
```
┌──(kali㉿kali)-[/etc/suricata/rules]
└─$ sudo nano cybersec.rules
```



```
┌──(kali㉿kali)-[/etc/suricata/rules]
└─$ cd ..

┌──(kali㉿kali)-[/etc/suricata]
└─$ ls
classification.config  reference.config  rules  suricata.yaml  threshold.config

┌──(kali㉿kali)-[/etc/suricata]
└─$ sudo nano suricata.yaml
[sudo] password for kali:

┌──(kali㉿kali)-[/etc/suricata]
└─$ cd rules

┌──(kali㉿kali)-[/etc/suricata/rules]
└─$ ls
app-layer-events.rules  dhcp-events.rules  files.rules        http-events.rules      modbus-events.rules  ntp-events.rules   smb-events.rules   stream-events.rules
cybersec.rules          dnp3-events.rules  ftp-events.rules   ipsec-events.rules     mqtt-events.rules    quic-events.rules  smtp-events.rules  tls-events.rules
decoder-events.rules    dns-events.rules   http2-events.rules kerberos-events.rules  nfs-events.rules     rfb-events.rules   ssh-events.rules
```

Ensure this file is referenced in the main configuration file:

```
/etc/suricata/suricata.yaml
```

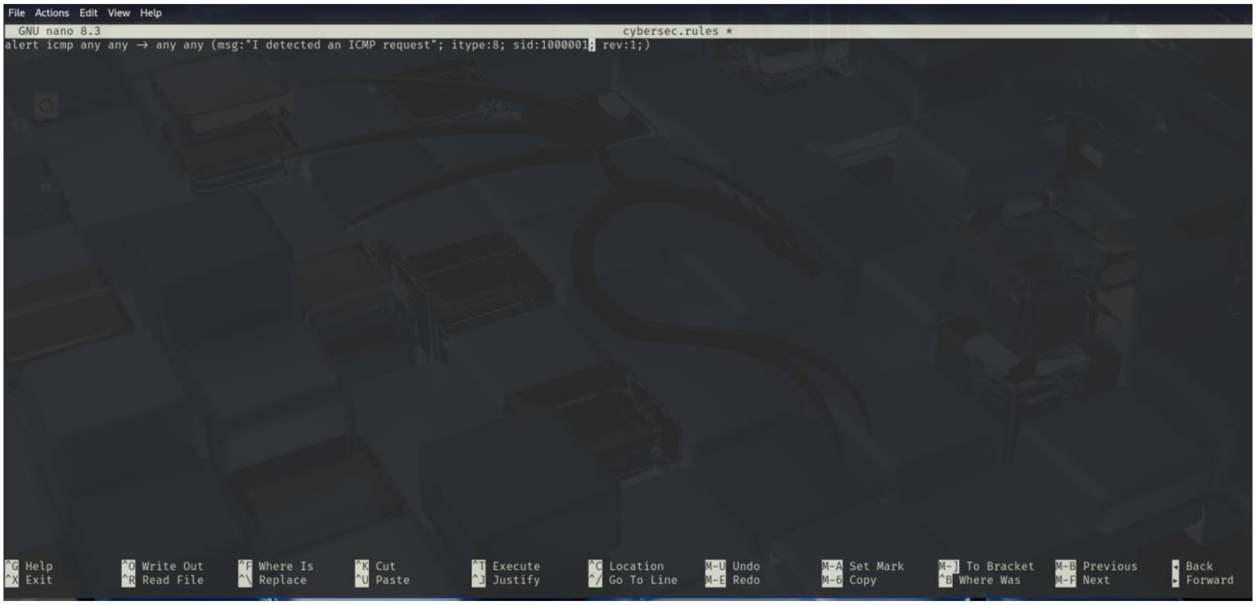


```
┌──(kali㉿kali)-[~]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -v
Notice: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 43030 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 43033 signatures processed. 1257 are IP-only rules, 4333 are inspecting packet payload, 37225 inspect application layer, 109 are decoder event only
Error: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
Warning: af-packet: eth0: AF_PACKET tpacket-v3 is recommended for non-inline operation
Info: runmodes: eth0: creating 1 thread
Info: unix-manager: unix socket '/var/run/suricata-command.socket'
Info: ioctl: eth0: MTU 1500
Notice: threads: Threads created → W: 1 FM: 1 FR: 1   Engine started.
^CNotice: suricata: Signal Received.  Stopping engine.
Info: suricata: time elapsed 167.501s
Info: counters: Alerts: 0
Notice: device: eth0: packets: 0, drops: 0 (0.00%), invalid chksum: 0
```

5. Adding a New Rule

Add a basic ICMP alert rule to detect ping traffic:

```
alert icmp any any -> any any (msg:"I detected an ICMP request"; itype:8;
sid:1000001; rev:1)
```



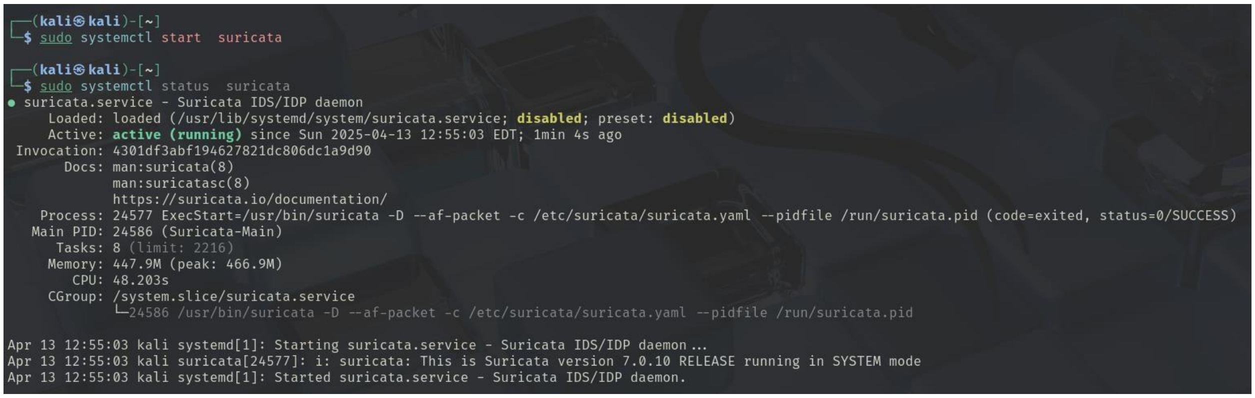
```
alert icmp any any → any any (msg:"I detected an ICMP request"; itype:8; sid:1000001; rev:1;)
```

This rule instructs Suricata to generate an alert whenever an ICMP packet is detected.

6. Starting the Suricata Service

Begin monitoring traffic using the correct network interface:

```
 sudo     systemctl     start
suricata
# OR sudo suricata -c /etc/suricata/suricata.yaml -i
eth0
```

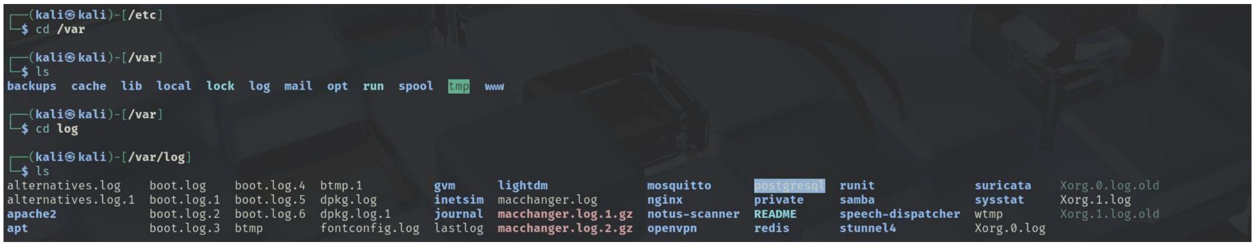


```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start  suricata

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status  suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
     Active: active (running) since Sun 2025-04-13 12:55:03 EDT; 1min 4s ago
 Invocation: 4301df3abf194627821dc806dc1a9d90
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 24577 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=exited, status=0/SUCCESS)
   Main PID: 24586 (Suricata-Main)
      Tasks: 8 (limit: 2216)
     Memory: 447.9M (peak: 466.9M)
        CPU: 48.203s
     CGroup: /system.slice/suricata.service
             └─24586 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Apr 13 12:55:03 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Apr 13 12:55:03 kali suricata[24577]: i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Apr 13 12:55:03 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```

7. Running Suricata

Confirm Suricata is running and parsing traffic:

```
/var/log/suricata/suricata.log
```



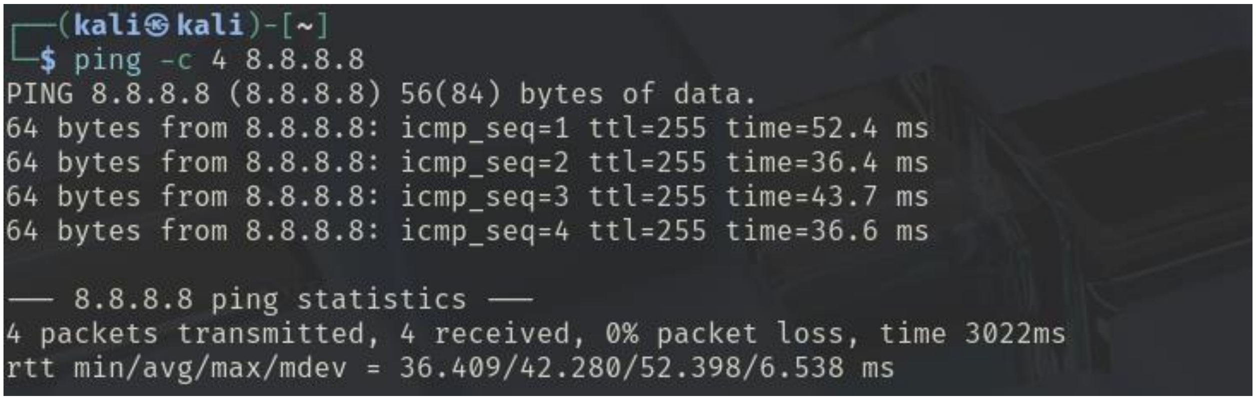
```
┌──(kali㉿kali)-[/etc]
└─$ cd /var

┌──(kali㉿kali)-[/var]
└─$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www

┌──(kali㉿kali)-[/var]
└─$ cd log

┌──(kali㉿kali)-[/var/log]
└─$ ls
alternatives.log    boot.log    boot.log.4  btmp.1          gvm      lightdm              mosquitto      postgresql  runit              suricata  Xorg.0.log.old
alternatives.log.1  boot.log.1  boot.log.5  dpkg.log        inetsim  macchanger.log       nginx          private     samba              sysstat   Xorg.1.log
apache2             boot.log.2  boot.log.6  dpkg.log.1      journal  macchanger.log.1.gz  notus-scanner  README      speech-dispatcher  wtmp      Xorg.1.log.old
apt                 boot.log.3  btmp        fontconfig.log  lastlog  macchanger.log.2.gz  openvpn        redis       stunnel4           Xorg.0.log
```

Watch for log entries indicating rule loading and live traffic capture.

8. Triggering the Alert

To verify that the custom rule is functioning, initiate traffic that matches the rule. For the ICMP rule:

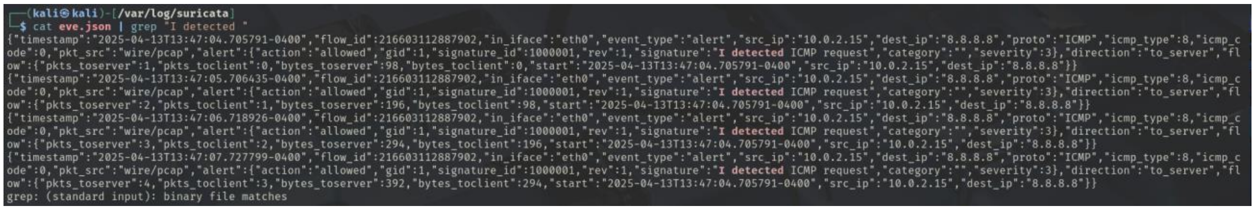
```
ping -c 4 8.8.8.8
```



```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=52.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=36.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=43.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=36.6 ms

—— 8.8.8.8 ping statistics ——
4 packets transmitted, 4 received, 0% packet loss, time 3022ms
rtt min/avg/max/mdev = 36.409/42.280/52.398/6.538 ms
```

9. Investigating the Alert

Review Suricata's alert log to confirm that the rule was triggered: **Example Output:**



```
┌──(kali㉿kali)-[/var/log/suricata]
└─$ cat eve.json | grep "I detected "
{"timestamp":"2025-04-13T13:47:04.705791-0400","flow_id":216603112887902,"in_iface":"eth0","event_type":"alert","src_ip":"10.0.2.15","dest_ip":"8.8.8.8","proto":"ICMP","icmp_type":8,"icmp_c
ode":0,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":1,"signature":"I detected ICMP request","category":"","severity":3},"direction":"to_server","fl
ow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":98,"bytes_toclient":0,"start":"2025-04-13T13:47:04.705791-0400","src_ip":"10.0.2.15","dest_ip":"8.8.8.8"}}
{"timestamp":"2025-04-13T13:47:05.706435-0400","flow_id":216603112887902,"in_iface":"eth0","event_type":"alert","src_ip":"10.0.2.15","dest_ip":"8.8.8.8","proto":"ICMP","icmp_type":8,"icmp_c
ode":0,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":1,"signature":"I detected ICMP request","category":"","severity":3},"direction":"to_server","fl
ow":{"pkts_toserver":2,"pkts_toclient":1,"bytes_toserver":196,"bytes_toclient":98,"start":"2025-04-13T13:47:04.705791-0400","src_ip":"10.0.2.15","dest_ip":"8.8.8.8"}}
{"timestamp":"2025-04-13T13:47:06.718926-0400","flow_id":216603112887902,"in_iface":"eth0","event_type":"alert","src_ip":"10.0.2.15","dest_ip":"8.8.8.8","proto":"ICMP","icmp_type":8,"icmp_c
ode":0,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":1,"signature":"I detected ICMP request","category":"","severity":3},"direction":"to_server","fl
ow":{"pkts_toserver":3,"pkts_toclient":2,"bytes_toserver":294,"bytes_toclient":196,"start":"2025-04-13T13:47:04.705791-0400","src_ip":"10.0.2.15","dest_ip":"8.8.8.8"}}
{"timestamp":"2025-04-13T13:47:07.727799-0400","flow_id":216603112887902,"in_iface":"eth0","event_type":"alert","src_ip":"10.0.2.15","dest_ip":"8.8.8.8","proto":"ICMP","icmp_type":8,"icmp_c
ode":0,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":1,"signature":"I detected ICMP request","category":"","severity":3},"direction":"to_server","fl
ow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":392,"bytes_toclient":294,"start":"2025-04-13T13:47:04.705791-0400","src_ip":"10.0.2.15","dest_ip":"8.8.8.8"}}
grep: (standard input): binary file matches
```

For detailed or structured logs (e.g., for SIEM ingestion), refer to:

```
/var/log/suricata/eve.json
```

10. Conclusion

This workflow demonstrates a successful Suricata deployment for basic threat detection. By installing and configuring Suricata, updating rules, adding a custom detection rule, and verifying alert functionality, I've built a foundation for further network defense. Suricata can now be expanded for full intrusion detection, threat hunting, and integration with tools such as ELK Stack, Splunk, or SIEM solutions.

Report Prepared by:

Aliu A. Sanusi

Cybersecurity Analyst